JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 307-319

ANALISIS PENGUJIAN KEAMANAN WEBSITE PENGELOLAAN INTERNET DESA KRAGAN MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)

Laila Fadila Burhani*[1)], Diah Priyawati[2)]
1. Universitas Muhammadiyah Surakarta, Indonesia
2. Universitas Muhammadiyah Surakarta, Indonesia

Article Info
Kata Kunci: keamanan; metode PTES; pengujian penetrasi; teknologi; website

Keywords: *penetration testing; PTES method; security; technology; website*

Article history:
Received 28 November 2023
Revised 12 December 2023
Accepted 26 December 2023
Available online 1 March 2024

DOI :
https://doi.org/10.29100/jipi.v9i1.4455

* Corresponding author.
Laila Fadila Burhani
E-mail address:
l200190261@student.ums.ac.id

ABSTRAK
Penggunaan teknologi pada era globalisasi saat ini telah membentuk ruang kehidupan baru sehingga menyebabkaan peningkatan pengguna aktif internet. Internet selain menghadirkan kemudahan bagi penggunanya, juga memberikan dampak negatif yang cukup berbahaya. Tingginya angka pengguna aktif internet seharusnya dibarengi dengan tingkat keamanan cyber yang tinggi. Akan tetapi, pada prakteknya kondisi keamanan cyber di Indonesia masih tergolong lemah. Menurut Pusat Operasi Keamanan Siber Nasional (Pusopskasinas) Badan Siber dan Sandi Negara (BSSN) mencatat hampir 1 milyar serangan cyber telah terjadi sejak januari hingga desember 2022. Oleh karena itu, untuk mengetahui kualiatas keamanan dan pentingnya fungsi serta performa yang ada pada website pengelolaan internet pada Desa Kragan, maka perlu diterapkan pengujian keamanan (penetration testing). Pengujian menggunakan metode Penetration Testing Execution Standard (PTES) yang merupakan panduan metodologi tentang apa yang diperlukan untuk uji penetrasi yang efektif. Hasil yang didapat setelah uji penetrasi testing yaitu terdapat 14 celah keamanan dimana beberapa celah diantaranya menjadi bahan untuk di eksploitasi. Celah keamanan tersebut yaitu Cloud Metadata Potentially Exposed, Absence of Anti-CSRF Tokens, SQL Injection, Missing Anti-clickjacking Header dan Vulnerable JS Library. Hasil SQL injection tidak dapat dilakukan karena website telah menggunakan Secure Socket Layer (SSL) untuk mendukung keamanan website, sedangkan hasil eksploitasi lainnya menunjukan bahwa celah keamanan tersebut berhasil dieksploitasi dan dapat menjadi ancaman cyber apabila tidak segera diperbaiki.

ABSTRACT
The use of technology in the current era of globalization has formed a new living space, causing an increase in active internet users. In addition to bringing convenience to its users, the internet also has a quite dangerous negative impact. The high number of active internet users should be accompanied by a high level of cyber security. However, in practice, cybersecurity conditions in Indonesia are still relatively weak. According to the Pusat Operasi Keamanan Siber Nasional (Pusopskasinas) Badan Siber dan Sandi Negara (BSSN), almost 1 billion cyber attacks have occurred from January to December 2022. Therefore, to determine the quality of security and the importance of functions and performance on the internet management website in Kragan Village, it is necessary to apply security testing (penetration testing). The test uses the Penetration Testing Execution Standard (PTES) method. The results obtained after the penetration testing test are 14 security gaps where some of them become material for exploitation. These security holes are Cloud Metadata Potentially Exposed, Absence of Anti-CSRF Tokens, SQL Injection, Missing Anti-clickjacking Header and Vulnerable JS Library. SQL injec- tion results cannot be carried out because the website has used Secure Socket Layer (SSL) to support website security, meanwhile other exploitation result show that the security gap was successfully exploited and can become a cyber threat if not immediately repaired.

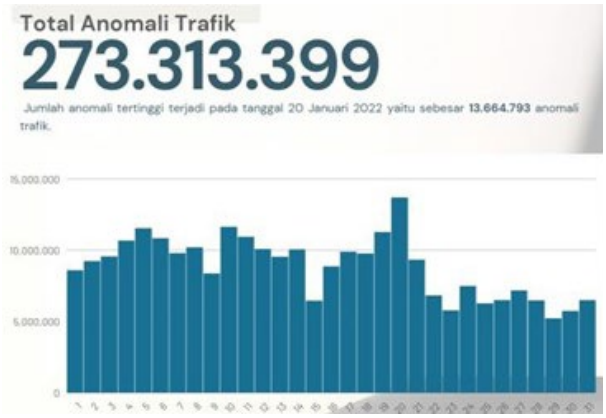
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 307-319

I. PENDAHULUAN

PENGGUNAAN teknologi pada era globalisasi saat ini telah membentuk ruang kehidupan baru dan bukan lagi merupakan hal yang asing ditemui ditengah-tengah masyarakat(Rizki, 2022). Penggunaannya pesat dalam berbagai aspek kehidupan salah satunya pemerintahan. Tata kelola pemerintahan semakin mudah dengan bantuan teknologi. Masyarakat dapat saling terhubung dengan memanfaatkan jaringan internet sehingga dalam penyelengaraan pelayanan publik dapat lebih terbuka, efektif, dan efisien(Nugraha, 2018).

Meningkatnya penggunaan internet selain menghadirkan kemudahan bagi penggunanya juga bersamaan dengan dampak negatif yang dimunculkan yaitu berupa ancaman keamanan. Berdasarkan data Internetworldstate, terdapat 212,35 juta atau 76.3% dari kesuluruhan populasi penduduk indonesia yang aktif menggunakan internet. Dengan jumlah tersebut indonesia menjadi negara urutan ketiga dengan pengguna internet terbanyak Asia.1

Menurut data yang disampaikan diatas, mayoritas masyarakat indonesia telah menjadikan internet sebagai pendukung untuk memenuhi kebutuhannya. Tingkat keamanan cyber harus ditingkatkan mengingat banyaknya pengguna aktif internet. Akan tetapi, pada prakteknya kondisi keamanan cyber di Indonesia masih tergolong lemah. Pusat Operasi Keamanan Siber Nasional (Pusopskasinas) Badan Siber dan Sandi Negara (BSSN) mendata hampir 1 milyar serangan cyber telah terjadi sejak Januari hingga Desember tahun 2022. Dalam laporannya, BSSN mencatat jumlah serangan cyber yang terjadi setiap bulan selama satu tahun dan yang tertinggi yaitu pada bulan Januari terpantau 273,3 juta serangan(Direktorat Operasi Keamanan Siber, 2022).



Gambar. 1. Jumlah serangan *cyber* Januari 2022

Berdasarkan data yang disajikan dalam gambar 1 dapat dikatakan bahwa Indonesia berpotensi menjadi negara target para hacker. Oleh karena itu, para pengembang sistem diharapkan lebih berhati-hati dan peduli terhadap kualitas keamanan website yang dibuat. Pemerintah khususnya Desa Kragan melalui Tim Informatika Universitas Muhammadiyah Surakarta membuat sebuah website yang digunakan untuk mengelola internet desa di bawah naungan Badan Usaha milik Desa (BUMDES). Website tersebut berfungsi untuk mengelola penggunaan internet desa, pembayaran internet dan keluhan layanan internet(Gunawan et al., 2022). Website dapat diakses oleh warga sebagai pengguna internet dan administrator yang ditunjuk oleh perangkat desa untuk mengelola segala urusan yang berkaitan dengan administrasi. Untuk menunjang proses pengelolaan yang terjadi dalam sistem, maka sangatlah penting melakukan pengujian keamanan untuk menghadapi tingginya ancaman cyber yang berdampak pada gangguan layanan dan kebocoran data

Penelitian tentang kualitas keamanan sistem sudah banyak dilakukan oleh peneliti sebelumnya menggunakan berbagai macam framework. Penggunaan framework bertujuan sebagai standart dalam pengujian keamanan sistem yang efektif. Salah satu penelitian dilakukan oleh(Ashari et al., 2022) yang melakukan pengujain pada website pemerintah kabupaten lampung barat. Pengujian dilakukan menggunakan framework Open Web Application Security Project (OWASP) dan mendapatkan hasil bahwa terdapat 53 URL yang rentan terhadap serangan Cross-site request forgery (CSRF). Akan tetapi tingkat resiko serangan yang terjadi pada website masih berada pada level rendah. Penelitian berikutnya dilakukan oleh (Sanjaya et al., 2020) yang melakukan pengujian pada lembaga pemilihan umum x sebagai situs website yang menyimpan data sensitif. Pengujian dilakukan menggunakan framework Information Systems Security Assessment Framework (ISSAF) dengan hasil pengujian diperoleh 18 celah keamanan yang terdapat pada website lembaga x dan 2 diantaranya terdapat celah keamanan yang berbahaya seperti SQL Injection dan Cross Site Scripting (XSS).

Framework lainnya yang digunakan dalam pengujian keamanan sistem yaitu *Penetration Testing ExecutionStandards* (PTES). Beberapa penelitian yang menggunakan *framework* PTES yaitu yang dilakukan oleh (Ningsih et al., 2021) pada kantor layanan terpadu pada pemerintah daerah XYZ. Pengujian dilakukan

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 307-319

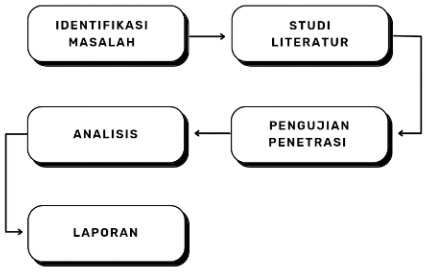
hingga tahap *vulner-ability assessement* dan menggunakan beberapa *tools* yaitu *OWASP ZAP, Acunetix,* dan *Paros*. Hasil penilaian kerentanan yang didapat yaitu memiliki tingkat risiko yang berbeda-beda sesuai dengan *tools* yang digunakan. Penelitian berikutnya dilakukan oleh (Dasmen et al., 2023) yaitu pengujian pada *e-learning* Universitas Bina Darma menggunakan alat *whois, reverse IP,* dan *nikto*.berdasarkan hasil penelitian dapat disimpulkan bahwa pengujian pada elearning2binadarma.ac.id teridentifkasi memiliki celah pada *Cross Site Scripting* (XSS) yang cukup berba- haya jika menyebar lebih jauh. Penelitian lainnya dilakukan oleh (Utoro et al., 2020) yang melakukan uji keamananpada aplikasi *website* milik SMKN 1 Cibatu. Pengujian lengkap dilakukan dari tahan *information gathering* hingga tahap *reporting*. Hasil pengujian yaitu mampu mengetahui tingkat kerentanan sistem paling tinggi yaitu *Cross SiteScripting, Cross Site Request Forgery* dan *Eavesdropping* yang sangat berpotensi mengakibatkan kebocoran pent-ing. Dari beberapa contoh penelitian yang sudah disebutkan diatas, pengujian keamanan sistem menggunakan metode PTES memiliki hasil analisis yang komprehensif. Selain itu metode PTES memiliki tahap-tahap pengujian yang lebih mudah dipahami oleh pengguna non-ahli(Syarif & Jatmiko, 2019).

Pada penelitian sebelumnya sudah pernah dilakukan uji keamanan sistem oleh (Priyawati et al., 2022) ter-hadap *website* pengelolaan internet Desa Kragan. Pengujian sistem dilakukan menggunakan metode *vulnerability assessment* (Priyawati et al., 2022) dimana metode tersebut hanya berfokus pada penilaian kerentanan sistem(Dewi& Setiawan, 2022) . Hasil analisis resiko dari metode *vulnerability assessment* hanya memberikan skor terhadap masing-masing kelemahan, sedangkan untuk mengambil langkah perbaikan, organisasi membutuhkan analisis yang lebih jelas.

Berdasarkan uraian di atas, penelitian ini akan mengevaluasi kembali kualitas keamanan *website* pengelolaan internet Desa Kragan menggunakan metode *penetration testing*(Utoro et al., 2020). Metode *penetration testing* melibatkan simulasi serangan dan memiliki hasil laporan tentang serangan yang berhasil dilakukan. Melengkapi penelitian sebelumnya yang hanya dilakukan hingga tahap *vulnerability assessment*, maka penulis melanjutkan penelitian hingga pada tahap *exploitation* dan *reporting*. Tujuan penelitian ini dilakukan yaitu untuk menentukan resiko keamanan yang mungkin terjadi dan menghasilkan bahan rekomendasi perbaikan untuk meminimalisir ter-jadinya serangan *cyber* pada *website* pengelolaan internet Desa Kragan.

II. METODE PENELITIAN

Sebagai pedoman untuk menunjang penulisan, penulis membuat alur proses dengan tujuan agar pembahasan lebih terarah dan tidak melebar. Adapun alur proses yang terjadi pada penelitian ini dijelaskan pada Gambar 2.



Gambar. 2. Alur proses penelitian

2.1 Identifikasi Masalah

Teknologi digunakan salah satunya dalam aspek layanan publik sehingga pelayanan untuk masyarakat jadi lebih efektif. Pelayanan berbasis teknologi menyebabkan makin meningkatnya penggunaan aktif internet. Ber- da-sarkan hal tersebut, teknologi dianggap selain memberikan keuntungan juga memberikan kerugian berupa an- ca-man keamanan. Website internet kragan merupakan sebuah website layanan publik untuk layanan internet desa yang menyimpan beberapa informasi pribadi. Oleh karena itu, pengujian keamanan untuk menilai kualitas website ini perlu dilakukan agar meminimalisir serangan cyber yang dapat terjadi sewaktu-waktu. Belum adanya pengujian keamanan menggunakan penetration testing menyebabkan penulis tertarik melakukan uji keamanan sebagai tema penelitian ini.Studi Literatur.

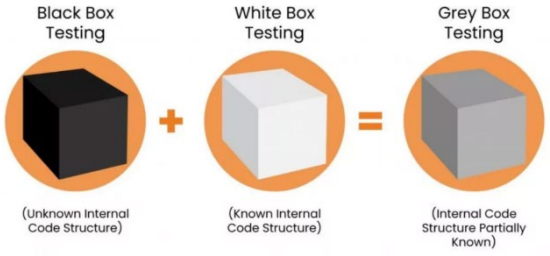
2.2 Studi Literatur

Studi Literatur dilaksanakan dengan mencari dan mengumpulkan informasi dari berbagai sumber yang berkai-tan dengan penelitian. Pada penelitian ini peneliti menggunakan berbagai sumber seperti e-book, jurnal, artikel

publikasi ilmiah, dan dokumen yang relevan. Studi literatur ini difokuskan dengan pencarian informasi tentang pengujian keamanan, metode yang digunakan, dan proses uji yang terjadi.

2.3 Pengujian Penetrasi (Penetration Testing).

Pengujian perangkat lunak memiliki tiga teknik yaitu black box, grey box, dan white box yang ditunjukkan pada Gambar 3. Penetration testing merupakan salah satu metode pengujian keamanan yang menggunakan teknik gray box. Teknik tersebut cocok dilakukan untuk uji penetrasi pada aplikasi web(Dhaifullah et al., 2022). Gray box testing merupakan kombinasi antara black box dan white box testing, jadi dalam pengujian berlangsung struktur internal atau kode hanya diketahui sebagian dan peneliti tidak perlu memiliki akses ke kode sumber. Peneliti hanya memanfaatkan bantuan alat pengujian perangkat lunak otomatis untuk mendapatkan kode.



Gambar. 3. Teknik *testing*

Penetration testing merupakan pengujian kerentanan keamanan untuk mendapatkan sebuah akses dalam sistem atau *website* yang berisi simulasi metode seolah-olah penyerang akan menerobos mekanisme keamanan sistem yang dituju untuk mendapatkan akses secara ilegal(Rosaliah et al., 2021). Pengujian keamnanan menggunakan metode *Penetration Testing Execution Standard* (PTES) yang merupakan panduan metodologi tentang apa yang diperlukan untuk uji penetrasi yang efektif(Utoro et al., 2020). Metode PTES dipilih karena dalam proses pengujian menggunakan tahap-tahap yang lebih mudah dipahami oleh pengguna non-ahli(Syarif & Jatmiko, 2019). Tahapan *PTES* terlihat pada Gambar 4.

Gambar. 4. Tahap *penetration testing.*

2.3.1 Information Gathering

Tahap ini adalah tahap untuk menentukan ruang lingkup dan tujuan pengujian keamanan. Untuk menunjang keberhasilan uji keamanan juga dibutuhkan informasi yang spesifik. Informasi yang dibutuhkan berupa analisis kebutuhan perangkat baik perangkat keras maupun perangkat lunak, informasi domain dan informasi jaringan. Informasi tersebut didapatkan menggunakan bantuan beberapa software pendukung.(Fauzan & Syukhri, 2021).

2.3.2 Threat Modelling

Suatu tahap menentukan model ancaman yang paling sesuai untuk memberikan eksekusi tepat pada pelaksanaan pengujian penetrasi. Pemodelan ini berfungsi untuk memudahkan penguji untuk memahami kerentanan keamanan yang akan ditemukan dalam pengujian. Model ancaman yang digunakan dalam PTES tidak khusus, tetapi membutuhkan model yang tetap kaitannya dengan representasi ancaman, kapabilitas, kualifikasi pada setiap organisasi yang diuji, serta kemampuannya untuk diaplikasikan pada pengujian di masa depan secara berulang dengan hasil yang serupa(Utoro et al., 2020).

2.3.3 Vulnerability Scanning

Proses pemindaian untuk menemukan celah keamanan dalam sistem dimana dapat menjadi sumber kelemahan yang dapat dieksploitasi. Pada penelitian ini, proses pemindaian menggunakan bantuan aplikasi OWASP ZAP. ZAP dari OWASP adalah salah satu yang direkomendasikan karena bersifat open source sehingga mudah dan gratis. ZAP mampu melakukan scan otomatis dari sistem target untuk menentukan bagian mana dari sistem tersebut yang rentan terhadap serangan cyber(Altulaihan et al., 2023)

2.3.4 Exploitation

Tahap eksploitasi yang berfokus pada celah keamanan untuk mengungkap kerentanan target. Hasil yang telah didapat pada tahap vulnerability scanning digunakan untuk melakukan eksploitasi(Ningsih et al., 2021). Tujuan tahap ini yaitu untuk memastikan seberapa besar potensi kerusakan yang dapat ditimbulkan sehingga penulis harus mencari tahu batasan pengujian kapan akan diakhiri untuk memastikan informasi sensitif tetap aman.

2.3.5 Reporting

Tahap terakhir dari metode PTES yaitu reporting yang berfungsi untuk melaporkan dokumentasi bagian-bagian penting pengujian. Dokumen berisi apa saja yang telah dilakukan selama pengujian beserta data yang diakses. Kemudian dokumen tersebut disusun menjadi sebuah informasi untuk dianalisis dan menghasilkan bahan perbaikan(Utoro et al., 2020)

2.4 Analisis

Tahap akhir dari penelitian ini yaitu analisis dan laporan. Proses penetration testing menghasilkan sebuah dokumen yang berisi hasil eksploitasi kerentanan yang telah dilakukan. Kemudian hasil tersebut dijabarkan dan dianalisis untuk mendapatkan solusi keamanan terbaik dan melindungi dari serangan dimasa mendatang.

2.5 Laporan

Keseluruhan penelitian yang sudah dilakukan kemudian dilaporkan pada tahap laporan. Dari hasil analisis sebelumnya ditarik kesimpulan untuk mendapatkan kemungkinan resiko yang dipat ditimbulkan dan digunakan untuk menentukan kualitas keamanan website. Laporan juga diberi saran-saran yang dapat digunakan untuk meningkatkan sistem.

III. HASIL DAN PEMBAHASAN

3.1 Information Gathering

Pengujian dilakukan terhadap *website* milik Desa Kragan. Langkah awal yaitu menentukan perangkat untuk menunjang keberlangsungan penelitian. Kebutuhan perangkat yang dibutuhkan yaitu perangkat keras dan lunak. Analisis kebutuhan perangkat ditunjukkan pada Tabel I

TABEL I
ANALISIS PENGUJIAN PERANGKAT

No	Parameter Pengujian	Spesifikasi
1	Laptop	HP 14 I3
2	RAM	4 GB
3	WiFi	Indihome
4	Sistem OperasiPenelitian	Windows 10
5	Information Gathering	Whois, Zenmap
6	Scanning	OWASP ZAP
7	Exploitation	SQLMap

Kemudian dilanjutkan untuk pengecekan domain dan jaringan. Pengecekan domain dilakukan menggunakan bantuan aplikasi whois. Whois merupakan sebuah *website* yang digunakan untuk mencari informasi seputar domain(Dasmen et al., 2023). Dari informasi yang didapat, *website* hanya menggunakan domain **"internetkragan.com".**Informasi tersebut ditunjukkan pada Gambar 5.

```
Domain Name: INTERNETKRAGAN.COM
Registry Domain ID: 2705171569_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.hostinger.com
Registrar URL: https://www.hostinger.com
Updated Date: 2023-06-21T05:45:58Z
Creation Date: 2022-06-20T12:59:39Z
Registrar Registration Expiration Date: 2023-06-20T12:59:39Z
Registrar: Hostinger, UAB
Registrar IANA ID: 1636
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibi
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientHold https://icann.org/epp#clientHold
Registry Registrant ID: Not Available From Registry
Registrant Name: Priyawati priyawati
```

Gambar 5. Hasil whois *"internetkragan.com"*

Setelah mendapatkan informasi tentang domain, selanjutnya adalah mencari informasi jaringan menggunakanaplikasi zenmap. Zenmap merupakan sebuah *tools* bersifat *open source* yang berfungsi untuk memindai port dan audit keamanan(Setiawan & Setiyadi, 2018). Hasil pengujian domain www.internetkragan.com mendapatkan in- formasi yang ditunjukkan pada Tabel II.

TABEL II
HASIL PENGUJIAN ZENMAP

No	Parameter Pengujian	Spesifikasi
1	Alamat IP	194.163.41.68
2	Port aktif bersifat open	21, 80, 110, 143, 443, 465, 587,993, 995, 3306
3	Sistem Operasi	Linux 4.9
4	Traceroute	Port 22/tcp
5	Service yang berjalan	ftp-data, ftp, ssh, rsftp, http, pop3,imap, https, smtp, spamassassin, mysql, ndmps.
6	DNS server yang digunakan	www.internetkragan.com -user srv147.niagahoster.com -PTR

3.1 Scanning

Penetration testing awalnya berlangsung secara manual dengan memanfaatkan kerentanan-kerentanan yang dieksplorasi, akan tetapi proses tersebut memakan waktu lebih panjang dan rentan terhadap kesalahan. Hingga seiring berkembangnya teknologi akhirnya muncul *Automatic Penetration Testing*(Railkar & Joshi, 2023). Proses yang akan dilakukan pada tahap ini yaitu pemindaian domain www.internetkragan.com menggunakan OWASP Zed Attack Proxy (ZAP) menu *Automatic Scanning*. Tujuannya yaitu untuk menemukan kelemahan yang ada da- lam *website.* Hasil proses *scanning* menggunakan OWASP ZAP dapat dilihat pada Tabel III.

TABEL III
HASIL *SCANNING* OWASP ZAP

No	Resiko	Jumlah
Cloud Metadata Potentially Exposed	Tinggi	2
SQL Injection	Tinggi	2
Absence of Anti-CSRF Tokens	Medium	20
Content Security Policy (CSP) Header Not Set	Medium	29
Cross-Domain Misconfiguration	Medium	45
Missing Anti-clickjacking Header	Medium	20
Vulnerable JS Library	Medium	5
Cookie without SameSite Attribute	Rendah	8
Cross-Domain JavaScript Source FileInclusion	Rendah	15
Server Leaks Information via "X-Powered-By" HTTP Response HeaderField(s)	Rendah	69
Server Leaks Version Information via "Server" HTTP Response Header Field	Rendah	1560
Strict-Transport-Security Header Not Set	Rendah	1560
Timestamp Disclosure – Unix	Rendah	27
X-Content-Type-Options HeaderMissing	Rendah	1546

Hasil *scanning* mendapatkan 14 celah keamanan teratas yang memiliki memiliki berbagai resiko seperti tinggi, medium, dan rendah. Resiko tersebut ditentukan otomatis oleh aplikasi OWASP berdasarkan *OWASP Top 10 2022*. *OWASP Top 10 2022* merupakan 10 kerentanan teratas tentang kerentanan sistem yang dibuat oleh or- ganisasi OWASP. Kemudian penulis menentukan untuk menganalisis beberapa celah keamanan yang memiliki level tinggi dan medium, karena celah tersebut lebih rentan terhadap serangan *cyber* dan memiliki resiko yang lebihserius. Penjelasan masing-masing celah tersebut diantaranya :

a. Cloud Metadata Potentially Exposed

Metadata berisi data lain tentang data yang mengandung informasi untuk dipakai dalam manajemen file suatu basis data. Metadata dibuat untuk menggambarkan data lain secara terperinci dan lengkap(Ul- rich et al.,2020). Semua penyedia layanan cloud menyediakan metadata melalui alamat IP yang tidak dirutakan dengan anggapan aman dari serangan luar. Akan tetapi, cara kerja serangan cloud metadata yaitu berupaya menyalahgunakan server NGINX yang salah konfigurasi untuk mengakses metadata ter- sebut. 169.154.169.254 merupakan IP yang dapat diekspos oleh server NGINX dan dapat diakses di bidang *header host*.[2]

b. SQl Injection

SQL Injection merupakan penyuntikan atau penyisipan kueri SQL dari klien ke aplikasi melalui input untukmendapat akses *database* (Lika et al., 2018). Injeksi SQL yang berhasil dapat membahayakan *database* karenamempengaruhi pelaksanaan perintah SQL yang telah ditentukan sebelumnya.

c. Absence of Anti-CSRF Tokens

*Cross Site Request Forgery (*CSRF) merupakan sebuah serangan eksploitasi *website* dimana identitas pengguna dipalsukan sehingga pengguna tanpa sadar mengirim sebuah permintaan ke *form* asli melalui *web-site* yang sedang digunakan. Kemudian *website* akan mengeksekusi permintaan dan dibawa pada sebuah *web-site* yang mengandung kode berbahaya(Ashari et al., 2022).

d. Missing Anti-clickjacking Header

Clickjacking adalah sebuah serangan menipu agar pengguna dapat mengklik elemen halaman *website* yangtidak terlihat atau samar sebagai elemen lain. *Clickjacking* dilakukan dengan menampilkan halaman atau ele-men HTML yang tidak terlihat, di bawah halaman yang dilihat pengguna(Ningsih et al., 2021). Dengan demikian, pengguna akan mengklik halaman yang terlihat tetapi sebenarnya mereka mengklik elemen yang tidak terlihat di halaman tambahan yang diubah urutannya.

e. Vulnerable JS Library

Pustaka *Jquery* yang teridentifikasi adalah versi 3.4.1 dimana versi tersebut rentan terhadap serangan. Ver-ifikasi dilakukan dengan mengecek respon dari aplikasi secara manual.

3.2 Gainning or Exploitation

a. SQL Injection

Implementasi *SQL injection* pada penelitian ini menggunakan metode *comment attack* dan *numeric SQL injection* (Kurnia, 2020). Metode *comment* dilakukan melalui proses *bypass.* Proses *bypass* merupakan jalan pintas yang memudahkan proses *login* karena tidak harus menggunakan *username* dan *password* yang ter- daftar. *Bypass* menggunakan *payload SQLI* yang sudah disiapkan sebelumnya agar dapat berhasil login. Apa-bila *payload* yang diinputkan sesuai, maka website berhasil diretas dan peneliti dapat memasukan kueri *SQL injection* (Djayali, 2020). Tabel IV berikut merupakan hasil uji injeksi SQL menggunakan metode *comment* yang dilakukan beberapa kali dengan hasil gagal terinjeksi.

TABEL IV
PAYLOAS SQLI

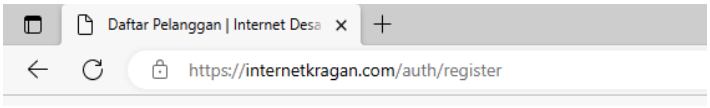
No	Username	Password	Hasil
1	'	'	Tidak Terinjeksi
2	=	=	Tidak Terinjeksi
3	' '	' '	Tidak Terinjeksi
4	'-'	'-'	Tidak Terinjeksi
5	' or " '	' or " '	Tidak Terinjeksi
6	' or true--	' or true--	Tidak Terinjeksi
7	or true--	or true--	Tidak Terinjeksi
8	' or 'x'='x	' or 'x'='x	Tidak Terinjeksi
9	or 1=1--	or 1=1--	Tidak Terinjeksi
10	' or 1=1/*	' or 1=1/*	Tidak Terinjeksi

TABEL IV
LANJUTAN PAYLOAD SQLI

No	Username	Password	Hasil
11	' or 1=1#	' or 1=1#	Tidak Terinjeksi
12	') or '1'='1	') or '1'='1	Tidak Terinjeksi
13	') or '1'='1--	') or '1'='1--	Tidak Terinjeksi
14	') or ('1'='1--	') or ('1'='1--	Tidak Terinjeksi
15	') or ('1'='1'/*	') or ('1'='1'/*	Tidak Terinjeksi

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 307-319

Bypass menggunkan metode *comments* tidak dapat menembus login karena *website* sudah menggunakan *encrypt* pada *password*. Injeksi SQL dapat dicegah menggunakan fungsi filter karakterdan enkripsi *password* yang ada pada form login(Kusdikdoyo & Widayanti, 2019). Selanjutnya pen- gujian dilakukan menggunakan metode *numeric, yaitu* dengan menyematkan karakter khusus seperti (:;-,=') dan kata kunci perintah pada parameter yang dikirim melalui URL di browser. Ciri-ciri *website* yang rentang terhadap injeksi yaitu yang masih memiliki ekstensi dan dapat diberi parameter setelah ekstensi pada urlnya kemudia *website* akan memberikan respon balik berupa respon *error*. Pengujian metode numeric dalam penelitian ini memanfaatkan SQLMap untuk mengakses *database*(Kurnia, 2020).

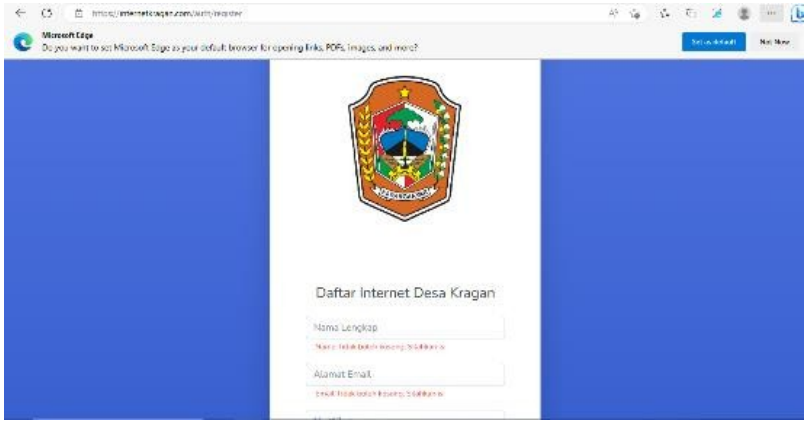


Gambar 6. Url register internet Desa Kragan

Gambar 6 terlihat bahwa ekstensi seperti .php pada url *website* internet kragan sudah tidak nampak. Kemudian penulis mencoba untuk menuliskan ekstensi pada url website yang ditunjukkan pada Gambar 7.

Gambar 7. Menambahkan ekstensi .php pada url

Gambar 7 menunjukan bahwa *website* tidak memberikan respon balik berupa respon *error*, *website* tetap memproses inputan sesuai dengan mestinya hasil inputan ditunjukkan pada Gambar 8.



Gambar 8. Hasil setelah penambahan ekstensi .php pada url

Setelah mengetahui bahwa *website* tidak memberikan respon balik berupa pesan *error*, penulis mencoba untuk melakukan akses *database* menggunakan bantuan *software* SQLMap. Proses injeksi SQL ditunjukkan pada Gambar 9.

Gambar 9. Hasil SQLMap

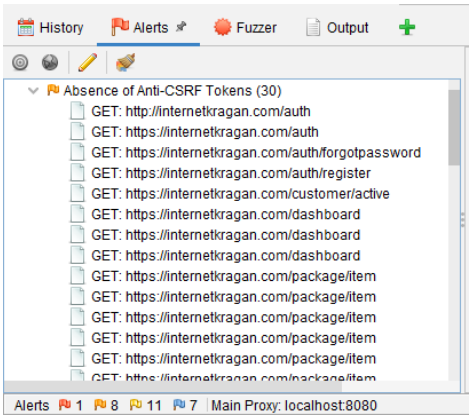
Mengacu pada Gambar 9, injeksi sql tidak dapat dilanjutkan karena www.internerkragan.com sudah menggunakan proteksi *Web Application Firewall (WAF)*. WAF merupakan suatu aplikasi *firewall* ber- basis *website* yang digunakan untuk memperkuat keamanan aplikasi. WAF melindungi dari eksploitasi dan seranganseperi *SQL injection* dengan cara memblokir *traffic* yang terindikasi memberi ancaman pada sistem(Dawadi et al., 2023)Selain itu website ini telah menerapkan *Secure Socket Layer (SSL)*. Hal

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 307-319

tersebut terlihat dari url yang sudah menggunakan HTTPS. *Website* yang telah memanfaatkan SSL akan lebih terlindungi dari pencu-rian data karena memiliki cara kerja enkripsi data pada setiap proses transfer (Utomo & Rokhmah, 2022), (Wahanani et al., 2020). Untuk membuktikan bahwa website sudah benar-benar memiliki sertifikat SSL yaitudapat melihatnya melalui *website* ssllabs.

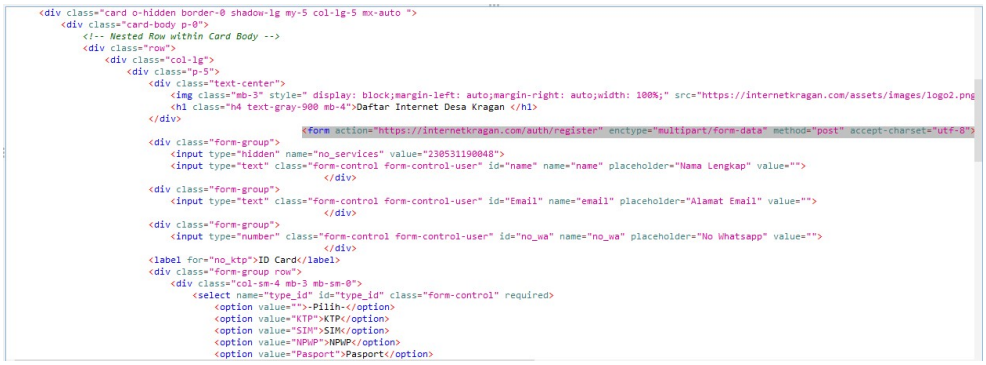
b. Absence of Anti-CSRF Tokens

Tujuan serangan CSRF adalah untuk memaksa pengguna mengirimkan permintaan perubahan sta-tus seperti mengubah kata sandi, mengunduh malware, atau mengunjungi situs berbahaya. CSRF menipu korban untuk menekan URL tidak sah yang dibuat secara jahat. Pemindaian dilakukanmenggunakan aplikasi OWASP ZAP pada domain http://internetkragan.com/ dan mendapatkan celah kea- manan CSRF seperti yang ditunjukan pada Gambar 10.



Gambar 10. Hasil pemindaian CSRF

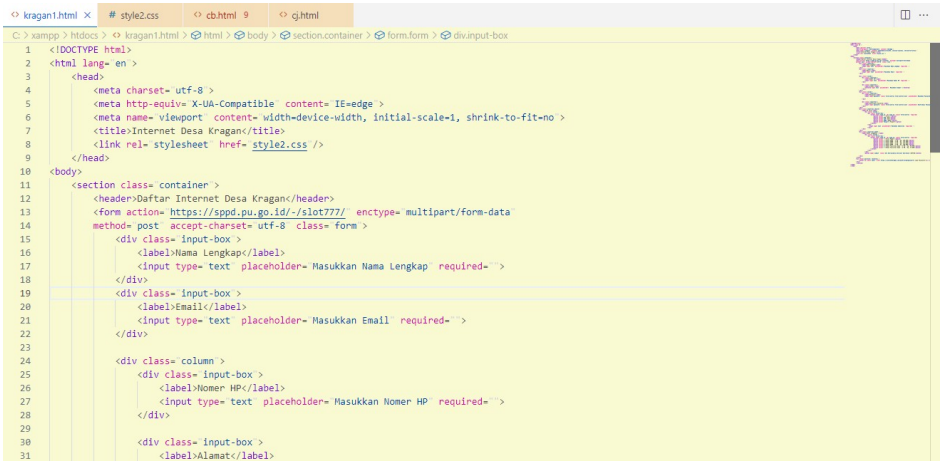
Gambar 10 diatas merupakan kumpulan dari beberapa *Uniform Resouce Locator (URL)* yang dipindai menggunakan OWASP ZAP. Pemindaian mendapatkan 30 celah dengan method GET dan POST.



Gambar 11. *Source code* asli

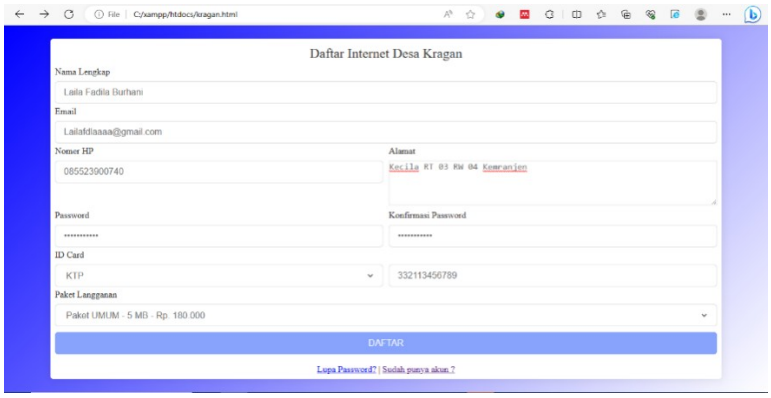
Gambar 11 merupakan *source code* asli yang dipilih untuk dieksploitasi. *Source code* ada pada *tag form* URL GET : https://internetkragan.com/auth/register. Dari *source code* pada gambar diatas, terdapat atribut *action* untuk menentukan URL tujuan dimana data dari suatu <form> akan diolah dan dikirimkan menuju URL yang didefinisikan. Jadi apabila tombol daftar ditekan, pengguna akan diarahkan ke laman yang sesuai dengan URL yang didefinisikan dalam kode.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 307-319



Gambar 12. *Output* tampilan

Gambar 12 merupakan merupakan *source code* yang dibuat menyerupai target untuk percobaan serangan CSRF. Eksploitasi dimasukkan pada atribut action untuk menentukan URL tujuan.



Gambar 13. *Output* tampilan

Gambar 13 merupakan tampilan hasil dari *source code* sebelumnya. Percobaan eksploitasi CSRF dimasukkan pada atribut action dengan mengganti perintah untuk mengunduh file zip.

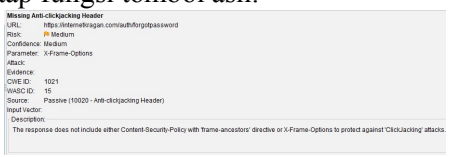
```
11    <section class="container">
12        <header>Daftar Internet Desa Kragan</header>
13        <form action="https://www.tutorialrepublic.com/examples/downloads/test.zip" enctype="multipart/form-data"
14        method="post" accept-charset="utf-8" class="form">
```

Gambar 14. *Source code* terinjeksi

Gambar 14 merupakan percobaan serangan CSRF yang dimasukkan pada atribut action dengan mengganti perintah untuk mengunduh folder zip. Apabila pengguna mengisikan form dan menekan tombol daftar, pengguna akan otomatis mengunduh sebuah file secara otomatis. Eksploitasi yang dilakukan disini tidak menggunakan file yang berbahaya, akan tetapi penyerang dapat memanfaatkan celah ini untuk disisipi sebuah URL yang otomatis mengunduh file atau aplikasi yang didalamnyamemuat *malware*.

c. Clickjacking

Cara kerja *clickjacking* biasanya menyembunyikan tombol asli dan menampilan tombol palsu yang lebih menarik, sehingga pengguna akan terkecoh dan menekan tombol palsu. Akan tetapi, saat tombol palsu ditekan,fungsi yang dijalankan tetap fungsi tombol asli.



Gambar 15. Hasil pemindaian *clickjacking*

Gambar 15 menunjukan bahwa celah keamanan clickjacking bisa dieksploitasi pada URL GET : https://internetkragan.com/auth/forgotpassword.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 307-319

Gambar 16. *Source code clickjacking*

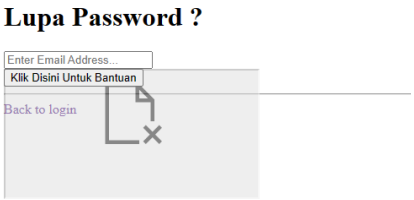
Gambar 16 menunjukan kode asli yang didapat dari hasil *vulnerability scanning* pada Gambar 16.

Gambar 17. Output tampilan

Gambar 17 menunjukan output tampilan dari *source code* pada Gambar 18. Pada laman bantuan lupa *pass-word*, terlihat adanya tombol "reset" dimana ketika tombol tersebut ditekan, maka *password* akan terganti. Untuk bisa melakukan *clickjacking*, perlu membuat tombol palsu diatas tombol "reset". menunjukan outputtampilan dari *source code* pada Gambar 20. Pada laman bantuan lupa *password*, terlihat adanya tom-bol "*reset password*" dimana ketika tombol tersebut ditekan, maka akan mendapatkan email berupatautan untuk menyetel ulang *password*. Untuk bisa melakukan *clickjacking*, perlu membuat tombol palsu untuk mengelabui pengguna.

Gambar 18. *Source code clickjacking*

Gambar 18 menunjukan *source code* yang didalamnya terdapat eksploitasi *clickjacking* berupa iframe dansebuah tombol dibelakang iframe. Iframe yaitu tag HTML untuk menampilkan sebuah *frame* yang berada didalam *frame* lainnya.[3]



Gambar 19. *Output* tampilan

Gambar 19 menampilkan hasil output apabila iframe tidak disamarkan. Tombol "*Reset Password*" sudah tertutup oleh tombol "Klik Disini Untuk Bantuan", akan tetapi apabila iframe tidak disamarkan, maka pengguna tidak akan terkecoh. Oleh karena itu *opacity frame* dibuat 0 sehingga tampilan iframe akan transparant.

Gambar 20. *Output* tampilan

Gambar 20 merupakan tampilan akhir dari percobaan *clickjacking*. Ketika pengguna menekan tom-bol "Klik Disini Untuk Bantuan", pengguna mengira akan mendapatkan sebuah bantuan tetapi tom-bol "*reset password*" akan mengirimkan URL ke *email* berupa tautan untuk menyetel ulang *pass- word* dimana

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 1, Maret 2024, Pp. 307-319

didalamnya terdapat *password* lama dan *password* baru. Pengguna akan terkecoh ka- rena menggangap akan mendapat bantuan tanpa menyetel ulang *password.*

Celah keamanan *clickjacking* merupakan kerentanan pada bagian *header*. Eksploitasi c*lickjacking* dibuat menggunakan metode *completely hidden.* Penulis membuat bingkai dari tag HTML berupa iframe untuk mengelabuhi pengguna melihat keseluruhan tampilan konten asli sehingga tindakan klik apapun akan mengarah ke konten yang tidak sesuai. Menyertakan *header HTTP X-Frame-Option* pada setiap halaman merupakan solusi yang cocok karena setiap halaman *website* sudah ter-*setting* untuk ditampilkan dalam bentuk*iframe* atau tidak.

IV. KESIMPULAN

Dari hasil pemindaian terdapat 14 celah keamanan dimana 3 diantaranya menjadi bahan eksploitasi. Ketiga celah keamanan tersebut yaitu *SQL injection*, *Missing Anti-clickjacking Header,* dan *Absence of Anti-CSRF To-kens*. Eksploitasi *SQL injection* tidak berhasil dilakukan karena *website* telah menerapkan keamanan yang cukup baik menggunakan WAF dan SSL. Akan tetapi, implementasi SSL saja pada *website* tidaklah cukup untuk mendapatkan kualitas keamanan yang unggul karena eksploitasi bisa berasal dari bagian mana saja. Tingginya angka serangan *cyber* yang terjadi beberapa tahun terakhir membuat para *developer* lebih peduli terhadap kea-manan *website* yang mereka buat. Pengujian keamanan atau *penetration* testing sudah banyak dilakukan salah satunya pada *website* pengelolaan internet Desa Kragan. Pengujian dilakukan menggunakan metode PTES dan mendapatkan hasil pemindaian yaitu terdapat 14 celah keamanan dengan level resiko tinggi, medium, dan rendah. Beberapa celah keamanan yang memiliki level tinggi dan medium menjadi bahan eksploitasi, karena celah ter-sebut lebih rentan terhadap serangan *cyber* dan memiliki resiko yang lebih serius Celah keamanan yang diek-sploitasi diantaranya C*loud Metadata Potentially Exposed, SQL injection*, *Absence of Anti-CSRF Tokens*, *Missing Anti-clickjacking Header,* dan *Vulnerable JS Library.* Eksploitasi *SQL injection* tidak berhasil dilakukan karena *website* telah menerapkan keamanan yang cukup baik menggunakan WAF dan SSL. Sedangkan beberapa celah keamnana lainnya berhasil diekspolitasi. Berdasarkan hasil pengujian keamanan tersebut, maka rekomendasi perbaikan dari temuan celah keamanan pada *website* pengelolaan inernet Desa Kragan dapat dirangkum seperti pada Tabel 5.

TABEL V
SARAN DAN REKOMENDASI PERBAIKAN

Parameter Pengujian	Spesifikasi
Cloud Metadata Potentially Exposed	Jangan menyimpan data pada konfigurasi NGINX yang tidak terkonfigurasi. Dalam *case* ini penggunaan variabel $host sudah diatur di header host, jadi segala tindakan dapat dikontrol penyerang.
Absence of Anti-CSRF To-kens	Jangan gunakan metode GET untuk permintaan apa pun yang memicu perubahan status. Dis-arankan menggunakan *framework Laravel* karena memiliki Anti-CSRF fitur karena berguna untuk mengantisipasi transmisi data dari luar situs web.
Missing Anti-clickjacking Header	Gunakan header *HTTP X-Frame-Option* pada se-tiap halaman.
Vulnerable JS Library	Tingkatkan ke versi terbaru jquery.
Cloud Metadata Potentially Exposed	Jangan menyimpan data pada konfigurasi NGINX yang tidak terkonfigurasi. Dalam *case* ini penggunaan variabel $host sudah diatur di header host, jadi segala tindakan dapat dikontrol penyerang.

Dari semua proses eksploitasi dan analisis dapat disimpulkan bahwa eksploitasi serangan terhadapcelah keamanan yang diperoleh dalam penelitian ini masih dalam level yang rendah dan kualitas kea- manan *website* berada pada level medium. Walaupun kualitas *website* tergolong baik, akan tetapi tetapsaja berbahaya apabila tidak segera diperbaiki dan berpotensi menjadi ancaman *cyber* yang merugikan instansi. Saran yang diberikan yaitu melakukan perbaikan terlebih dahulu terhadap celah keamanan yangtelah dianalisis dan apabila perbaikan telah dilakukan, pengujian selanjutnya baru bisa dilakukan agar celah keamanan yang didapat akan lebih minimum. Untuk pengujian selanjutnya, diharapkan menggunakan metode berbeda agar kualitas keamanan *website* pengelolaan internet Desa Kragan semakin meningkat.

DAFTAR PUSTAKA

[1] M. Rizki, "POLITEIA : Jurnal Ilmu Politik Perkembangan Sistem Pertahanan / Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi," vol. 14, no. 1, pp. 54–62, 2022.
[2] S. Tentang and E. Sukses, "E-GOVERNMENT DAN PELAYANAN PUBLIK E-GOVERNMENT DI PEMERINTAH KABUPATEN SLEMAN)," pp. 32–42.
[3] R. A. Hanneman, "Daftar Isi Daftar Isi :," pp. 2–5, 2009.
[4] I. F. Ashari, V. Oktarina, R. G. Sadewo, and S. Damanhuri, "Analysis of Cross Site Request Forgery (CSRF) Attacks on West Lampung Regency Websites Using OWASP ZAP Tools," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 11, no. 2, pp. 276–281, 2022, doi: 10.32736/sisfokom.v11i2.1393.
[5] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *ojs.unud.ac.idI Sanjaya, GMA Sasmita, DMS ArsaJurnal Ilm. Merpati, 2020•ojs.unud.ac.id*, Accessed: Jul. 24, 2023. [Online]. Available: https://ojs.unud.ac.id/index.php/merpati/article/download/61232/35784
[6] S. W. Ningsih, A. Almaarif, and A. Widjadjarto, "Vulnerability Testing Analysis of XYZ Regional Government Site Using PTES," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 3, pp. 1543–1556, 2021, doi: 10.35957/jatisi.v8i3.1224.
[7] R. N. Dasmen, T. L. Widodo, and M. Tio, "PENGUJIAN PENETRASI PADA WEBSITE ELEARNING2 . BINADARMA . AC . ID DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD)," vol. 11, no. 1, pp. 91–95, 2023, doi: 10.35508/jicon.v11i1.9809.
[8] S. Utoro, B. A. Nugroho, and S. R. Widianto, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," vol. 6, no. 2, pp. 169–178, 2020.
[9] J. D. No, "ANALISIS PERBANDINGAN METODE WEB SECURITY PTES , ISSAF DAN OWASP DI DINAS KOMUNIKASI DAN INFORMASI KOTA BANDUNG Universitas Komputer Indonesia".
[10] D. Priyawati, S. Rokhmah, C. Utomo, J. Slamet, and R. No, "Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP," vol. 03, no. 03, 2022.
[11] B. Tasya and K. Dewi, "Kajian Literatur : Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web," 2021.
[12] S. Testing and E. Survey, "Survei Teknik Pengujian Software," vol. 2, no. 1, pp. 31–38, 2022.
[13] Y. Rosaliah, J. Jayanta, B. H.- Senamika, and undefined 2021, "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx," *conference.upnvj.ac.id*, 2021, Accessed: Oct. 11, 2022. [Online]. Available: https://conference.upnvj.ac.id/index.php/senamika/article/view/1572
[14] O. Access, "Web vulnerability analysis and implementation," pp. 0–8, 2018, doi: 10.1088/1757-899X/407/1/012081.
[15] A. Scanner, T. Analysis, and A. A. Website, "Jurnal Mantik," vol. 4, no. 2, pp. 1138–1144, 2020.
[16] H. Ulrich *et al.*, "Understanding the Nature of Metadata – A Systematic Review Table of Contents," 2020.
[17] T. Jaringan, "InfoTekJar : Jurnal Nasional Informatika dan Analisis Forensik Serangan SQL Injection dan DoS Menggunakan Instrution Detection System Pada Server Berbasis Lokal," vol. 2, pp. 0–4, 2020.
[18] A. D. Djayali, "Analisa Serangan SQL Injection pada Server pengisian Kartu Rencana Studi (KRS) Online," vol. 1, no. 1, pp. 16–24, 2020.
[19] E. T. Pelangi, "Menerapkan Aspek Keamanan Database Pada Website," vol. 2, pp. 419–430.
[20] S. N. Nida and D. Purnamasari, "Implementasi Web Application Firewall dan Penetration Testing pada Web Server," 2005.
[21] F. Y. Fauzan and Syukhri, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang dari keamanan web adalah sebanyak 96 dengan disimpulkan Acunetix Threat Level 2 yaitu pada level Medium yang artinya tidak," *J. Vocat. Tek. Elektron. dan Inform.*, vol. 9, no. 2, 2021, [Online]. Available: http://ejournal.unp.ac.id/index.php/voteknika/article/download/111778/105248
[22] I. C. Utomo, S. Rokhmah, T. Informatika, and U. M. Surakarta, "Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta," vol. 6, no. 2, pp. 143–150, 2022.
[23] U. J. I. Coba, S. Man, I. N. The, M. Pada, K. Ssl, and P. Http, "UJI COBA SERANGAN MAN IN THE MIDDLE PADA," vol. 13, no. 1, pp. 21–26, 2020.